(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 286 267 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
26.02.2003 Bulletin 2003/09

(51) Int Cl.7: G06F 12/02, G06F 12/08

(21) Application number: 01119923.9

(22) Date of filing: 17.08.2001

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: Sony International (Europe) GmbH
10785 Berlin (DE)

(72) Inventor: Dinescu, Dan,
c/o Sony International (Europe) GmbH
85609 Aschheim-Dornach (DE)

(74) Representative: Körber, Martin, Dipl.-Phys. et al
Mitscherlich & Partner
Patentanwälte
Sonnenstrasse 33
80331 München (DE)

(54) **Flash based non-volatile memory**

(57) A mobile communication device comprises volatile memory means (202), non-volatile memory means (201) and control means (100), whereby the control means (100) store data in the volatile memory (202) and periodically flush said data out the volatile memory (202) into the non-volatile memory (201). At least a part of the non-volatile memory is divided into two sectors (204) and the control means (100) sign one of the sectors (204) as an active sector (204a) by a sequence counter displaying a greater value than the sequence counter of the other sector (204b). The control means (100) flush the data into the other sector (204b) being labeled as inactive in case of the control means (100) erased this inactive sector (204b) already and the data in the volatile memory (202) has changed as from last flushing. Subsequently the control means (100) form an incremented sequence counter in the now active sector (204a).

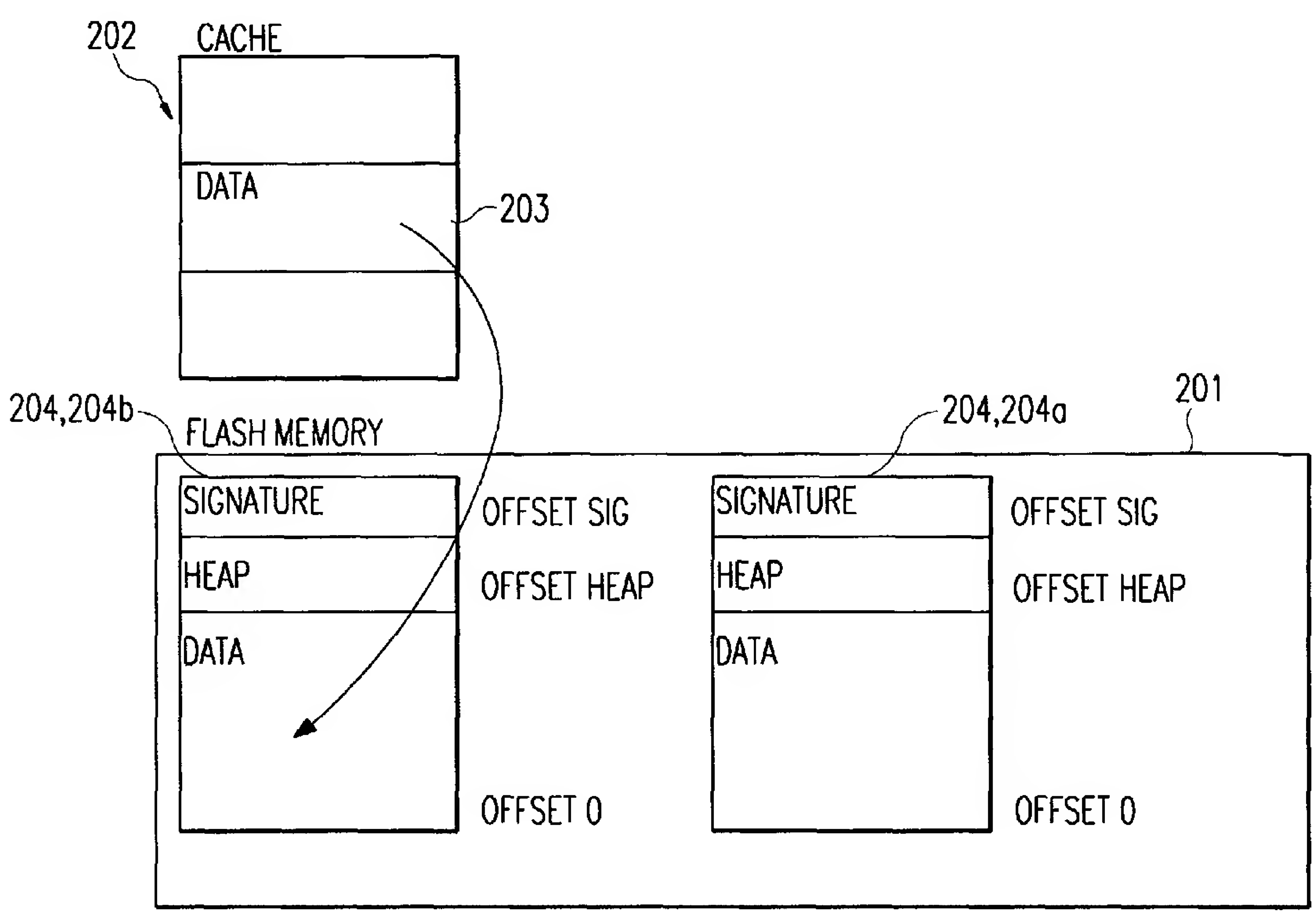

Fig. 2

EP 1 286 267 A1

Description

[0001] The present invention relates to a mobile communication device and a method of operating such a mobile communication device.

[0002] A mobile communication device, e.g. a mobile phone, needs a non-volatile memory to store software and parametric data. Parametric data are for example adjustment data of displays, telephone books and login data of a telephone network carrier. The non-volatile memories do not require power to be supplied to them in order to maintain data. Certain types of non-volatile memories can be erased and occupied with new data without a special-purpose device. The content of the memory can be erased and new data can be stored on the memory device being integrated in the circuit. However, the number of erasing-cycles of these non-volatile memory devices is limited and there is the danger of failure over lifetime of a mobile phone. On the other hand, it is desired to use as little different types of memory devices as possible to save costs and to increase the working speed of the mobile communication device. An intelligent management of storing and erasing data is required.

[0003] EP 0 834 882 A2 discloses a memory management method comprising storing parametric data in a volatile memory, such as RAM, and periodically updating the data stored in the RAM to a non-volatile memory such as a Flash Memory. Updating data to the Flash Memory is dependent on the time since the last update or on the importance of the data in the RAM. The parametric data is stored in dependence on the nature of the data, for reducing wear of the non-volatile memory. The method is, e.g. applied to a mobile phone and the information of the data may relate to the user interface setup, the user personal telephone directory, or some other parameters of the radiotelephone, that vary during use.

[0004] In a second realization EP 0 834 882 discloses a method of managing a memory device, wherein data is distinguished in data of different priority levels and the period of storing the data in the non-volatile memory is dependent on the priority level. Data is stored into the non-volatile memory in a linked list.

[0005] A disadvantage of the methods described above is that there are no arrangements to ensure a data recovery in case of an unexpected power failure. A further disadvantage is that the linked list always stores the complete set of information. The consumption of storage space is relatively great and an erasing of storage space is often required. This increases the wear of a non-volatile memory, notably a FLASH memory.

[0006] DE 197 50 525 C1 discloses a method that relates to the data management in a vehicle. The vehicle comprises a computer with a RAM memory and a FLASH memory. At deactivation of the vehicle and thereby of the data management system, data is stored into the FLASH-memory. Upon restoring the power supply, the data, which had to be maintained, is read out from the non-volatile memory and stored into the volatile memory. Data storing in the non-volatile memory is organized by a circulating storing method. The data is repeatedly stored and only one set of data is actual. At the start in a first phase, default values are transferred into non-volatile memory to quickly ensure the ability of the vehicle to work. In a second phase, the newest set of data is read out from the non-volatile memory and the default values are overwritten with that.

[0007] Disadvantageously the disclosed method cannot be protected against data loss in case of an unexpected failure of power supply, without the possibility to execute a special "going down" method. In general, the method is not set to ensure the maintenance of security sensitive data as login data of a telephone network carrier.

[0008] The present invention aims to avoid a third type of memory in a mobile communication device and to enable the use of a non-volatile memory with a limited number of erasing cycles in a mobile communication device for maintaining data records, which change during usage of a mobile communication device, whereby an acceptable lifetime of the mobile communication device without a lifetime failure has to be ensured.

[0009] The above object is achieved by a mobile communication device according to claim 1 and a memory managing method according to claim 17. In a mobile communication device according to the present invention volatile memory means, non-volatile memory means, and control means (control circuit and/or control program) are provided. The control means advantageously is a control program, but can also be a control circuit. The control means store data in the volatile memory and periodically flush said data from the volatile memory into the non-volatile memory, whereby at least a part of the non-volatile memory is divided into two sectors and the control means label one of the sectors as an active sector by a sequence counter displaying a greater value than the sequence counter of the other sector and the control means flush the data into the other sector being labeled as inactive if the control means had already erased this inactive sector and if the data in the volatile memory has changed since a last flushing, whereby the control means subsequently increment the sequence counter of the former inactive sector to become the new sequence counter of the now active sector.

[0010] The mobile communication device of the present invention has the advantage to avoid a third type of a non-volatile memory while guaranteeing secure storage of data and preventing lifetime failure of the mobile communication device within an acceptable period of time. The number of erasing procedures is limited by the period of time until the next storing. Considering the expected lifetime of a mobile communication device the period can be determined so that the number of erasing procedures does not wear the non-volatile memory by more then the maximum possible erasing cycles. The

sequence counter always gives the newest data set. After power on, the control means can discover the actual data set. In case there was no change in data being stored in the volatile memory, this data will not be flushed. This feature additionally reduces the wear of the non-volatile memory. This arrangement avoids the need of a third type of memory. Normally there is one volatile memory like a RAM and two kinds of non-volatile memories.

[0011] Further, preferably, the control means distinguish normal data and secure data. The control means immediately store secure data in the non-volatile-memory when said data was changed.

[0012] In case of loosing data, the disadvantages and the dangers differ depending on the kind of data. Certain sets of parameters are security sensitive data as login data of the telephone network carrier, for example. The distinction of types of data can specifically reduce the risk of data loss.

[0013] In case the mobile communication device is not turned off as provided but a breakdown of power supply occurs, the kind of data, that is most sensitive about data loss, is protected as far as possible.

[0014] The control means may store secure data, which were changed between periodical flushing, in a heap area of the active sector as a patch of the outdated information in a data area. The patch is containing at least the information about offset, length of the outdated information and the new information itself.

[0015] This feature reduces the number of sector erasures, because only the information is stored which is necessary to be maintained at all. The total set of data does not normally require the entire sector. A part of the sector can be built as a heap area. The patches of the sets of the secure data having been changed are stored in the heap area. Also it is not possible to overwrite a small part of a non-volatile memory at a single memory address without having erased at least a relating block of the memory before, it is always possible to store in an area having been remained free up to now. The amount of erasing cycles is lowered, because secure data normally requires less space and a flushing is avoided by storing patches of the outdated secure data.

[0016] Further, preferably, the control means store data, which are changed while flushing the data of the volatile memory into the non-volatile memory, as a patch of the outdated information in another area of the volatile memory. The patch contains at least information about offset, length of the outdated information and the new information itself. The control means change normal data in the volatile memory after the flushing is completed according to the patch and store a patch of secure data in the heap of the active sector of the non-volatile memory.

[0017] Upon the flushing there may occur the problem of data, which are just being flushed into the non-volatile memory, being changed. To obtain consistent data records, the changes of data are not immediately processed but the data sets are stored as patches in a different area of the volatile memory. When the flushing is completed, the patches of normal data are used to overwrite the data in the volatile memory with the correct and updated information. The patches of secure data are copied to the heap area of the then active sector in the non-volatile memory. The offset of the patch is adapted to point to the correct data record. That minimizes the risk to get inconsistent data. Data, which have changed, cannot be mixed with unchanged data and thereon cannot be flushed into the non-volatile memory causing data loss by discrepancies or by not noticeable combinations of new and old information.

[0018] Further, preferably, the control means initiate an erase procedure over the then inactive sector after flushing the data into the now active sector.

[0019] In a preferred embodiment of the invention, the control means check byte by byte if the then inactive sector was actually erased.

[0020] Thereby the protection against the false storing of data is improved. The concurrence of a not erased bit and a bit, which should not be set by storage, may cause a wrong information.

[0021] In an embodiment optionally the erase procedure can be suspended while performing and can continue. The period of time for periodically flushing and erasing may be at least 15 minutes.

[0022] Erasing requires a long time and should be interruptible to execute other processes. The period of not less than 15 minutes implies an estimated lifetime of e. g. at least about 5½ years under normal conditions of use of a mobile phone.

[0023] Further, preferably, one bit of the sequence counter is always clear and the sequence counter is of an eight bit type having the first bit always clear. The control means test, whether the sequence counter of the one sector is greater than the sequence counter of the other sector or vice versa by equalizing the one sequence counter to the incremented other sequence counter modulo 128 or vice versa.

[0024] There are non-volatile memory types, for example a FLASH-memory, which are cleared in the state of all the bits being set. By incrementing a sequence counter may become the value "FF" equal to an erased address. The described feature prevents from that.

[0025] In a preferred embodiment, the control means store in the new active sector a check sum computed over the sequence counter and over four identification bytes of the active sector after flushing. The control means test the validity of the active sector by the checksum and in case of failure uses the other sector as an active sector. The control means can use default values copied to the volatile-memory in case of the second sector being invalid, too.

[0026] A power supply failure could occur while flushing or erasing. The embodiment of the invention always ensures a valid data record, either stored in an active sector or given by default values.

[0027] In case of switching on the mobile communication device after power off, said control means copy the information of the data in the active sector into the volatile memory.

[0028] This embodiment facilitates a fast read/write access to the data, because all the time since power on there is a copy of the data in the volatile memory. The time of accessing to the volatile memory is short in proportion to that of the non-volatile memory.

[0029] Preferably the non-volatile memory is a FLASH-type one and the control means display a message in case of three or more failed attempts to erase a sector.

[0030] This feature gives notice to a user of the mobile communication device that the device needs service. The memory failure is a defect not expected or noticeable by the user. On that score a message is advantageous.

[0031] A preferred application of the invention comprises a mobile communication device with a FLASH-memory as the non-volatile memory.

[0032] The method according to the present invention (memory managing method) is to be applied by a mobile communication device, which comprises a volatile memory, a non-volatile memory, and control means. The method at least includes the steps of storing data in the volatile memory and of periodically flushing said data from the volatile memory into the non-volatile memory by the control means. In a further step it is tested by the control means, which of the two sectors in the non-volatile memory is an active one having a sequence counter with the greater value and which is an inactive one having a sequence counter with the lower value. In a further step it is tested by the control means, whether the data in the volatile memory has been changed since last flushing by the control means. The data in the inactive sector is flushed by the control means if the inactive sector is already erased. A sequence counter, which has an incremented value in relation to the sequence counter of the previous active sector, is stored into the now active sector by the control means.

[0033] The method fundamentally has the same advantages as the mobile communication device. Furthermore, a realization of the method is often simple, because no or less modifications of hardware are required. There are remarkable numbers of mobile phone types with a FLASH memory as the only non-volatile memory. The method can ameliorate the management of safe storing of data in an easy way. Advantageously, the inventive method is realized in a software program being able to perform the method steps when stored in a memory of a mobile communication device.

[0034] Further, preferably, at the inventive memory managing method normal data and secure data are distinguished by the control means and furthermore said secure data is stored in the non-volatile memory by the control means immediately in case of being changed.

[0035] A favorable method furthermore comprises the step of storing secure data being changed between periodical flushing into a heap area of the active sector as a patch of the outdated information in a data area by the control means, wherein at least information about an offset, a length of the outdated information and the new information itself is contained.

[0036] Data being changed while flushing the data of the volatile memory into the non-volatile memory, may be stored as a patch of the outdated information into another area of the volatile memory by the control means, said patch containing at least information about an offset, length of the outdated information and the new information itself. Said data being normal data is changed in the volatile memory according to the patch after flushing having been completed. A patch of the secure data is stored in the heap of the active sector of the non-volatile memory after flushing having been completed.

[0037] Preferably, the then inactive sector is checked by the control means byte by byte if it is actually erased.

[0038] Favorably the erase procedure is suspended by the control-circuit, when another software-procedure has to be executed and the continuation of the erasure procedure is initiated by the control unit after the software-procedure has been completed.

[0039] Data may be flushed and the inactive sector may be erased by the control means at a minimum period of 15 minutes.

[0040] Suitably the sequence counter is of an 8 bit type having one bit always clear and it is tested by the control means, whether the sequence counter of one sector is greater than the sequence counter of the other sector or vice versa by equalizing the one sequence counter to the incremented other sequence counter modulo-128 and vice versa.

[0041] A check sum computed over the sequence counter and over four identification bytes of the new active sector can be stored in the new active sector by the control means. While proceeding a "switch on" starting procedure, the validity of the active sector is tested by the control means making use of the check-sum and in case of an invalid active sector, the other sector is used as an active sector. In case of the other sector being invalid, too, default values are copied to the volatile memory by the control means.

[0042] After switching on the mobile communication device the information of the data in the active sector patched by the heap-information is copied into the volatile memory.

[0043] The methods described above are suitably used with a FLASH-memory as the non-volatile memory and a message is displayed in case of three or more failed attempts to erase a sector.

[0044] A preferred embodiment in accordance with the present invention will now be described with references to the accompanying drawings in which:

Fig. 1 shows a block diagram of a microcontroller in a mobile phone,

Fig. 2 schematically shows the volatile memory map and the FLASH-memory map of an inventive mobile phone,

Fig. 3 schematically shows a cutout of the FLASH-memory map containing information labeled as signature in Fig. 1,

Fig. 4 schematically shows an information unit stored in the FLASH-memory in Fig. 2 at the area labeled as heap,

Fig. 5 shows a flow chart for a routine, useable for storing and flushing in accordance with the inventive method,

Fig. 6 shows a flow chart for a routine, which runs if data has been changed just now,

Fig. 7 shows a flow chart for a subroutine of the flow chart in Fig. 5, useable for flushing, and

Fig. 8 shows a flow chart for a subroutine of the flow chart in Fig. 5, useable for a power-on process.

[0045] A preferred embodiment of the present invention will be described with reference to the accompanying drawings.

[0046] Fig. 1 shows a block diagram of a mobile phone as an example of a mobile communication device with control means 100 having a multiplicity of integrated on-board operating units. The control means 100 comprise a central processing unit (CPU) 101, a random access memory (RAM) 102, a FASH-memory 103, input/output drivers 104, and a digital signal processor (DSP) 105, which is a sophisticated functional unit, e.g. to compute voice coding. The FLASH-memory 103 provides non-volatile memory means and also replaces EEPROM type memory means in the present embodiment of the invention, which will be explained in detail further below. A second type of memory is typically used on board of the microcontroller as the control means 100. That memory is the RAM 102 providing a volatile memory means for use in association with any software running in the microcontroller and itself being stored in the RAM 102 or storing data in the RAM 102. The input/output drivers 104 handle transfer of data between the units of the control means 100 and devices of the mobile phones as microphone, loudspeaker, and receiver/antenna. The CPU 101 is coordinating all the operating units described above and interacting with these.

[0047] Fig. 2 is a view on a schematic map of a volatile memory 202, for example the FLASH-memory 103 of Fig. 1, and of a volatile memory 202 consisting of the RAM 102 of Fig. 1, e.g. A mobile phone as a specific type of a mobile communication device uses both memories 201,202 in its control means 100. The view presents the logical arrangement of the memories 201,202. The separated numbers of addressable storage units, which are allocated to a logical unit, are clarified by a rectangle for each logical unit. The volatile memory 202 contains a data area 203. In this data area 203 a complete set of data is stored containing the information about normal data and secure data. Normal data in general are all data, which can change according to settings of a user or a radio network carrier. Secure data are settings, which can change and are of importance for a faultless operating of the mobile phone. Such data are adjustment data and parameters, such as login or network protocol information. The complete set is copied from the non-volatile memory 201 into the volatile memory 202, when the power supply is switched on and the mobile phone is used. As a result, the information is always available in the volatile memory 202 and therefore it is possible to read it quickly. The two sectors 204, 204a, 204b do not necessarily require the total storage space of the non-volatile memory 201. Other blocks may contain the working or operating software of the mobile phone, which is not changing besides in case of a software update.

[0048] The FLASH-memory 103 is parted in at least two sectors 204. The physical design of a FLASH-memory 103 is composed of blocks of memory addresses of the same number.
One or more of these blocks are bunched together to a sector 204 and called correspondingly in the context of the present invention. The concrete implementation uses a single block of 8KB for each sector 204. One of the sectors 204 is marked as an active sector. Following and by convention, the sector 204 on the right is the active sector 204a and the other sector on the left is the inactive sector 204b. The roles of the active sector 204a and the inactive sector 204b continuously exchange and the current arrangement relates to a single state of the inventive method. Each sector is logically parted again in three parts. The first part is a signature. The last and third part is a data area, respectively. Between these two parts the second part is arranged as a heap. The composition of the signature will be explained further below with reference to Fig. 3. The data area serves to receive and maintain data, which is flushed from the data area of the volatile memory 202 into the inactive sector 204b. It contains both the normal data and the secure data after flushing in the state they have been in the data area of the volatile memory 202. Addresses of data records are indicated with an offset, which is a relative address, referring to the beginning or the first absolute address of the sector. The numeration is ascending in direction of the end of the sector or with higher absolute addresses.

[0049] Fig. 3 schematically shows a cutout of the FLASH-memory 103 map containing information labeled as signature in Fig. 2. The signature consists of fixed check data and a sequence number having a length of one byte and a check sum having a length of one byte. The control means 100, as shown in Fig. 1,

compute the check sum over the sequence counter and over four identification bytes of the active sector. After flushing the result is stored in the signature of the then active sector 204a. The active sector 204a is marked with a sequence counter of a greater value, i.e. by the sequence counter of the other sector incremented with a value "1".

[0050] Fig. 4 schematically shows an information unit stored in the FLASH-memory 103, 201 in Fig. 2 at the area, which is labeled as heap. The information unit is a patch used to store the change of secure data immediately without flushing all the content of the data from the volatile memory 202 into the non-volatile memory 201. The patch consists of a data length information having a length of one byte. Said byte is followed by two bytes comprising the data offset and as a third essential part of the patch by the changes of the data themselves. The main part of the patch consists of this data area in general. The omissions of the rectangle indicate the normally larger quantity of the data in the data area in relation to the three bytes.

[0051] The control means 100 flush the data area 203 of the volatile memory 202, when the period of time is lapsing and an erasing subroutine has already erased the inactive sector 204b. The control means 100 copy the data from the data area 203 of the volatile memory 202 into the data area of the inactive sector 204b. This shows the arrow 205, symbolizing the movement of copied data. In a second step, the control means 100 increment the sequence counter of the active sector by the value "1", except if it would then become a "FF", a byte with all bits set. In this case the sequence counter is set to the value "00". Furthermore, the control means 100 compute a check sum over the new sequence counter value and over four identification bytes of the sector. When the sequence counter is now greater than the sequence counter of the up to now active sector 204a and the check sum indicates that the procedure of flushing is completed, the up to now active sector 4a and the inactive sector 204b exchange their roles. An erasing procedure can run over the up to now active sector 204a, as the new inactive sector.

[0052] With reference to Fig. 5 a program flow will be explained, which is running at all the time a mobile communication device is operating and which realizes the inventive method in a mobile phone. The routine controls the flushing. In a first step after a start 501, that is reached during a power-on of the mobile phone as an example of a mobile communication device, a subroutine "power on" 502 is called. The subroutine "power on" 502 will be explained in more detail with reference to Fig. 7 further below. The routine itself, furthermore by convention named "main routine" is a part of the software of the mobile phone. The main routine enters its state "start" 501 at any time upon activation of the mobile phone, when the software calls the main function. After the subroutine "power on" 502 is completed there is a complete set of data in the data area 203 of the volatile memory 202. The control means 100 and especially the software of the mobile phone can quickly access the data. The main routine now enters a step 503, which is a decision whether the preset period of time lapsed. The period is set to e.g 15. minutes. In case of "no" (period of time not yet lapsed) the process reaches a further decision step "heap full?" 506. Unless the heap is full the process returns to the decision 503 until the result is "yes" (period of time has lapsed). Alternatively the process proceeds to the predefined process "flushing" 505 as a subroutine. which will be explained with reference to Fig. 7 in more detail further below. This ring forms a wait modus to ensure a flushing not earlier than after e. g. 15 minutes and the main routine is at least active in the wait modus, when the mobile phone is powered on. That means the routine is periodically activated by an interrupt for example and then the routine executes the decision 503 and the ring as long as a time scheduling of the control means 100 or an overflow of the heap stops the execution. In case of "yes" at the decision 503 the process flow enters a further decision step "data dirty?" 504. When no data changed in the data area 203 of volatile memory 202, a new period of time starts and the process flow returns to the wait modus and the decision 503 without doing anything else, because the data at the data area 203 and in the active sector 204a are identical to each other. In case the data have been changed, the decision "data dirty" results in "yes" and the predefined process step "flushing" 505 is called as a subroutine. When the process step "flushing" 505 is completed the main routine proceeds to a predefined process step 703 "erase inactive sector" and finally returns into the wait modus and to the decision step 503.

[0053] This implementation of the invention advantageously improves the security against lifetime failure of the mobile phone and at same time the security against data loss. A period of about 15 minutes results in lifetime of about five and a half years. The length of the period, however, can be set different depending on the specific application and/or the particular device.

[0054] Furthermore, there is an exit-procedure, which is not shown. This procedure secures a data flushing during an intended power going down of the mobile phone. In case of data in the volatile memory 202 being dirty and the period of time not having lapsed, the exit-procedure flushes data in the non volatile 201 memory .

[0055] With reference to Fig. 6 a flow chart for a routine will be explained, which runs if data have just been changed. As an external event, for example phone book entries by an user or settings of a network carrier, data are changed, which can be normal or secure data. In this case the process flow enters the state data input "changing of data" 601. When data are changed other software e.g. calls the main process as a subroutine. In the decision "flushing at same time" 602 the process flow differs dependent on whether a subroutine "flushing" 505 called by the main process is running at the same time. This is necessary to avoid the storing of

wrong data or mixed data. The main process, which is activated by an interrupt and determines the lapse of the period, and the current process can concur. More in detail, the subroutine "flushing" 505 can run, if activated by the main process. Due to time scheduling the process "flushing" can get a data record, partly changed over again by the current process. From that fact the decision 602 leads to the action "store patch in volatile memory" 603 in case of "yes". A patch equal to the patch explained above is stored in another area of the volatile memory. It contains information about the offset, the data length, and the changed data itself. The main process subsequently can determine the addresses of data in the data area 3 of the volatile memory 202, which are not up to date yet again, by the offset. After storing the patch in RAM and, if secure data, in the heap of the actual sector, the current process enters a step "return" 607 in a direct way and is terminated. In a step "changed data secure data" 605a is tested whether the data needs an immediate storing in the non-volatile memory 201. In case of "no" as result of the previous decision 602 the action 604 occurs "storing changes in data area". The changed data overwrites the data in the data area 3 of the volatile memory 202. In the next step the process flow gets to the decision "changed data secure data" 605 where it is tested whether the changed data are secure data, i.e. if the data need an immediate storing in the non-volatile memory 201. In case of "yes", the action executes "store patch in heap of active sector" 606. The changes of the secure data are stored into patches as described above. The patches are written to the heap area of the non-volatile memory 201. If there is no space in an embodiment of the invention it is possible to provide an extraordinary flushing. In the following step the process flow of the process reaches the step "return" 607 and is terminated. Normal data are stored into the non volatile memory 201 by the main process after the period of time lapsed.

[0056] With reference to Fig. 7 the predefined process "flushing", which is called as part of the main process in step 505, will be explained. The figure shows a flow chart for the subroutine. The subroutine process is activated with its start step 701, when called by the main process of Fig. 4. The first step is a decision 702, whether the at the moment inactive sector is already erased. A FLASH-memory 103 as an example for a used non-volatile memory 201 is erased, when all bits are set to the value "high". If a bit is not set by a write action and is still set to the value "low", by other words, the bit is not erased, a data write mistake occurs. To protect against that, the decision 702 tests, whether an erasing process is already completed. In case of "no" a predefined process 703 "erase inactive sector" is called. The flow chart of the process 703 is not shown. It is essential that the erasing process checks bit by bit that the memory addresses are actually erased before itself returns to the main process of Fig. 5. If the inactive sector is surely erased, the "flushing" process proceeds to a step, formed by an action 704 "copy data area to data area of the inactive sector". This step follows the action "build sequence counter and check sum" 705. The sequence counter is formed from the sequence counter of the active sector 204a, which is incremented. In case it would become the value "FF", the count starts with the value "0" again. The check sum is computed over the new sequence counter and four predefined bytes and is stored into the signature of the sector 204b as shown in Fig. 2.

[0057] The flushing process now enters the decision "data changed while flushing" 706. As shown in Fig. 6 and explained above with reference to state 602 of Fig. 6, it can occur that data have changed during the flushing process. These changes were stored into patches. The decision tests, whether such patches exist and if the decision results in "no" the flushing process reaches the termination point "return" 707.

[0058] In case of "yes" at step 706 an action "overwrite" 708 corrects the data in the data area 203 of the volatile memory 202 by the patches stored in another area of the volatile memory 202. After that, the decision "secure data changed" 709 tests, whether one of the patches relates to secure data. If the decision 709 results in "yes" the action "transfer" 710 starts. It copies the patches of secure data into the heap area of the new active, former inactive sector 4b. The offsets of these patches are adapted to the addresses of corrected data in the data area of the sector 4b of the non-volatile memory 201.

[0059] The danger of secure data loss is advantageously eliminated in case of a sudden power supply failure. Secure data is always stored in the actual sector as a patch in the heap.

[0060] Fig. 8 shows a flow chart for a subroutine of the flow chart in Fig. 5, useable for flushing. The predefined process is the step 502 of the main process in Fig. 5. The process executes at any time, immediately after power on. The start 801 "power on" is followed by the action 802 "select one sector". The action randomly selects one of the at least two sectors 204 in the non-volatile memory 201. Next, the process enters the decision 803 "sequence counter greater than other". If it results in "no", the sequence counter of the chosen sector 204 is less than that of the other sector 204, the action 804 "select other sector" starts. It exchanges the selection of sectors 204 and the other one becomes the selected sector 204. The process proceeds to a decision 805 "valid check sum?". This decision computes the expected check sum and equalizes its value with the stored check sum of the sector 204. In case that the decision 805 results in "yes", the process reaches action 806 "copy data into volatile memory". A copy of the data in the volatile memory 202 enables the control means 100 of the device to access data quickly. The process now terminates at step 807 "return". In case that the decision 805 results in "no", the process reaches action 808, which exchanges the selection of sectors 204 and the respective other one becomes the selected sector 204.

The functionality is equal to the function of step 804. The new selected sector is tested by a decision 809 "valid checksum?", which has an identical functionality with decision 805. If the decision 809 results in "yes" the process proceeds to action 806 and furthermore proceeds as described above. In case of a "no" the process enters an action 810 "copy default data into volatile memory". To ensure under all circumstances the operability of the mobile phone, in case of no valid sector, default values are used. At last the process terminates with step 807.

[0061] Advantageously the process makes available the optimal set of data, which can be recovered. The mobile phone can always access the data at the volatile memory 202, when switched on. Since in case of total data loss a limited ability to operate is ensured.

Claims

1. Mobile communication device comprising volatile memory means (202), non-volatile memory means (201) and control means (100), whereby the control means (100) store data in the volatile memory (202) and periodically flush said data from the volatile memory (202) into the non-volatile memory (201),
characterized in,
that at least a part of the non-volatile memory is divided into two sectors (204) and the control means (100) label one of the sectors (204) as an active sector (204a) by a sequence counter displaying a greater value than a sequence counter of the other sector (204b) and the control means (100) flush the data into the other sector (204b) being labeled as inactive if the control means (100) had already erased this inactive sector (204b) and if the data in the volatile memory (202) has changed since a last flushing, whereby the control means (100) subsequently increment the sequence counter of the former active sector (204a) to become the sequence counter of the now active sector (204b).

2. Mobile communication device according to claim 1,
characterized in,
that the control means (100) distinguish normal data and secure data.

3. Mobile communication device according to claim 2,
characterized in,
that the control means (100) immediately store secure data in the non-volatile-memory (201) when said data has been changed.

4. Mobile communication device according to claim 3,
characterized in,
that the control means (100) store secure data, which was changed between periodical flushing, in a heap area of the active sector (204a) as a patch of the outdated information in a data area, containing at least information about off-set, length of the outdated information and the new information itself.

5. Mobile communication device according to claim 4,
characterized in,
that the control means (100) store data, which is changed meanwhile flushing the data from the volatile memory (202) into the non-volatile memory (201), as a patch of the outdated information in another area of the volatile memory (202), containing at least information about off-set, length of the outdated information and the new information itself, and if flushing has been completed, the control means (100) change normal data in the volatile memory (202) according to the patch and store a patch of secure data in the heap of the active sector (204a) of the non-volatile memory (201).

6. Mobile communication device according to one of claims 1 to 5,
characterized in,
that the control means (100) initiate an erasing procedure (703) over the now inactive sector (204b) after flushing the data into the now active sector (204a).

7. Mobile communication device according to claim 6,
characterized in,
that the control means (100) check byte by byte if the inactive sector (204b) was actually erased.

8. Mobile communication device according to claim 6 or 7,
characterized in,
that the erase procedure can be suspended while running and can continue.

9. Mobile communication device according to one of claims 1 to 8,
characterized in,
that the period of time for periodically flushing and erasing is at a minimum 15 minutes.

10. Mobile communication device according to one of claims 1 to 9,
characterized in,
that one bit of the sequence counter is always clear.

11. Mobile communication device according to claim 10,
characterized in,
that the sequence counter is of eight bit type having the first bit always clear and the control means (100) test whether the sequence counter of the one sector (204) is greater than the sequence counter of the other sector (204) or vice versa by equalizing the one sequence counter to the incremented other se-

quence counter modulo-128 or vice versa.

12. Mobile communication device according to one of claims 1 or 11,
characterized in,
that after flushing the control means (100) store in the new active sector (204a) a check sum computed over the sequence counter and over four identification bytes of the active sector (204a) and in case of switching on the mobile communication device after power off, said control means (100) test the validity of the active sector (204a) by the check-sum and in case of failure use the other sector (204b) as an active sector.

13. Mobile communication device according to claim 12,
characterized in,
that the control means (100) use default values copied to the volatile-memory if the second sector (204) is invalid, too.

14. Mobile communication device according to one of claims 1 to 13,
characterized in,
that upon start of the device the control means (100) copy the data from the active sector (204a) into the volatile memory (202).

15. Mobile communication device according to one of claims 1 to 14,
characterized in,
that the non-volatile memory (201) is a FLASH-type (103) one.

16. Mobile communication device according to one of claims 1 to 15,
characterized in,
that the control means (100) display a message in case three or more attempts failing to erase a sector.

17. Memory managing method applied by a mobile communication device with a volatile memory (202), a non-volatile memory (201) and control means (control circuit and/or control program) (100) comprising the steps:

storing data in the volatile memory 202 and periodically flushing said data from the volatile memory (202) into the non-volatile memory (201) by the control means (100);

characterized by the steps:

testing by the control means (100) which of two sectors (204) in the non-volatile memory (201) is an active one (204a) having a sequence counter with the greater value and an inactive one (204b) having a sequence counter with the lower value;
testing by the control means (100) whether the data in the volatile memory (202) has changed as from last flushing by the control means(100);
flushing the data in the inactive sector by the control means (100) in case the inactive sector has already been erased.
storing an sequence counter in the now active sector (204a) by the control means (100), whereby the sequence counter is the sequence counter of the old active sector been incremented with the value "1".

18. Memory managing method according to claim 17, furthermore comprising the step of distinguishing normal data and secure data by the control means (100).

19. Memory managing method according to claim 18,
characterized in,
that changed secure data is immediately stored in the non-volatile memory (201) by the control means (100).

20. Memory managing method according to claim 19,
characterized in,
that secure data being changed intermediate periodical flushing is stored in a heap area of the active sector (204a) as a patch of the outdated information in the data area by the control means (100), wherein at least information about an off-set, a length of the outdated information and the new information is contained.

21. Memory managing method according to claim 20,
characterized in,
that data being changed meanwhile flushing the data of the volatile memory (202) into the non-volatile memory (201), is stored as a patch of the outdated information in another area of the volatile memory (202) by the control means (100), said patch containing at least information about off-set, length of the outdated information and the new information, and that normal data is changed in the volatile memory (202) according to the patch and that a patch of secure data is stored in the heap of the active sector (204a) of the non-volatile memory (201), after flushing is completed.

22. Memory managing method according to one of claims 17 to 21,
characterized in,
that an erase procedure over the now inactive sector (204b) is initiated by the control means (100) after flushing.

23. Memory managing method according to claim 22, **characterized in,** **that** the then inactive sector (204b) is checked byte by byte whether being actually erased by the control means (100).

24. Memory managing method according to claims 22 or 23, **characterized in,** **that** the erase procedure (703) is suspended by the control-circuit, when another software-procedure must run and when the software-procedure has been completed the continuation of the erasure procedure is initiated by the control unit.

25. Memory managing method according to one of claims 22 to 24, **characterized in,** **that** at the earliest all 15 minutes the data is flushed and the inactive sector is erased by the control means (100).

26. Memory managing method according to one of claims 17 to 25, **characterized in,** **that** one bit of the sequence counter is always clear.

27. Memory managing method according to claim 26, **characterized in,** **that** the sequence counter is of eight bit type and it is tested by the control means (100), whether the sequence counter of the one sector (204) is greater than the sequence counter of the other sector (204) or vice versa by equalizing the one sequence counter to the other incremented sequence counter modulo-128 and vice versa.

28. Memory managing method according to one of claims 17 to 27, **characterized in,** **that** a check sum is computed over the sequence counter and over four identification bytes of the new active sector (204a) and is stored in the new active sector (204a) by the control means (100) and after switching on the mobile communication device the validity of the active sector (204a) is tested by the control means (100) making use of the check-sum and in case of a invalid active sector (204a) the other sector (204b) is used as an active sector (204a)

29. Memory managing method according to claim 28, **characterized in,** **that** default values are copied to the volatile memory (202) by the control means (100) if the other sector (204b) being invalid, too.

30. Memory managing method according to claim 29, **characterized in,** **that** the information of the data in the active sector (204a) is copied into the volatile memory (202) by the control means (100).

31. Memory managing method according to one of claims 17 to 30, **characterized in,** **that** a FLASH-memory (103) is used as the non-volatile memory (202).

32. Memory managing method according to one of claims 17 to 31, **characterized in,** **that** a message is displayed in case of three or more failed attempts to erase a sector (204).

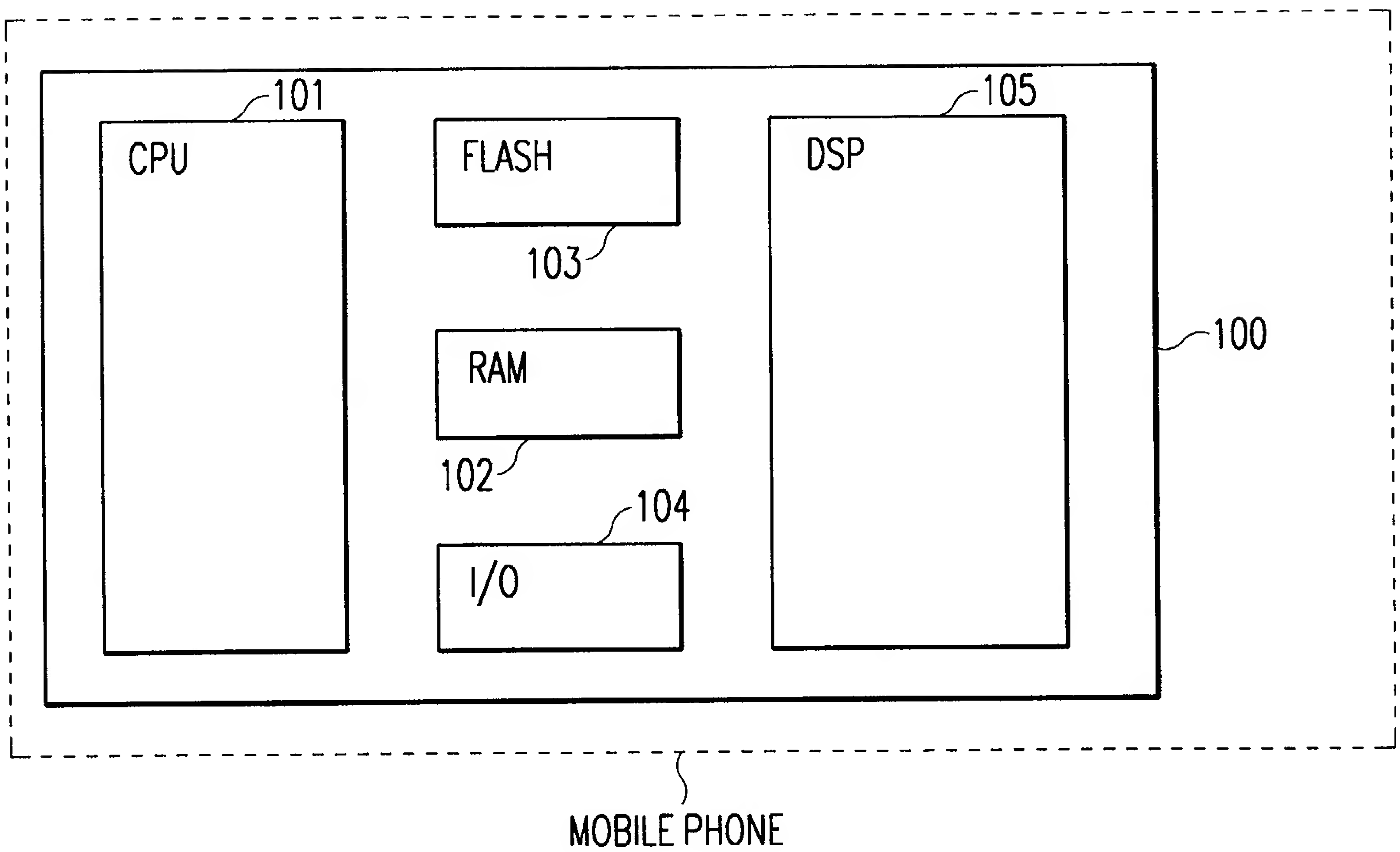

Fig. 1

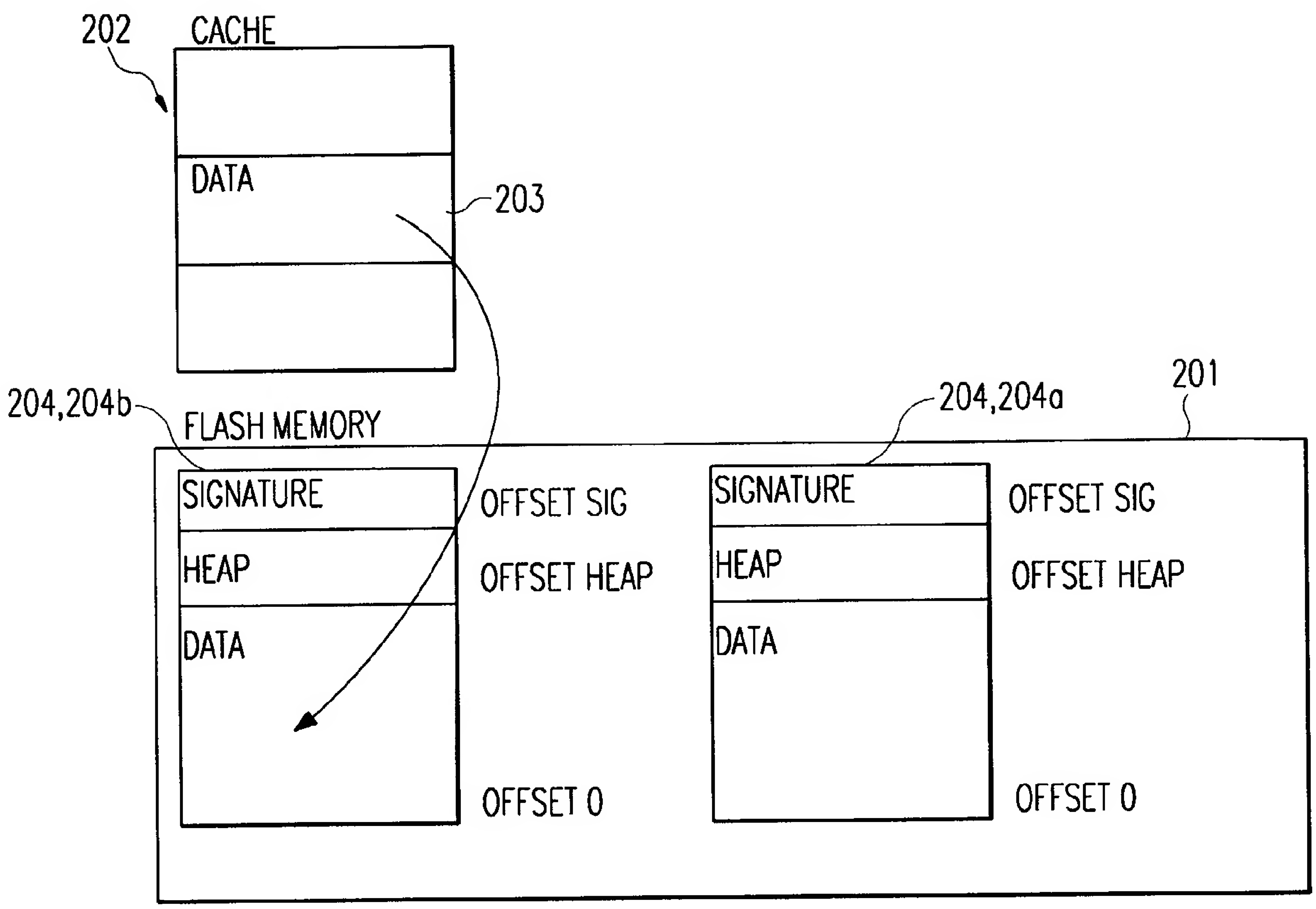

Fig. 2

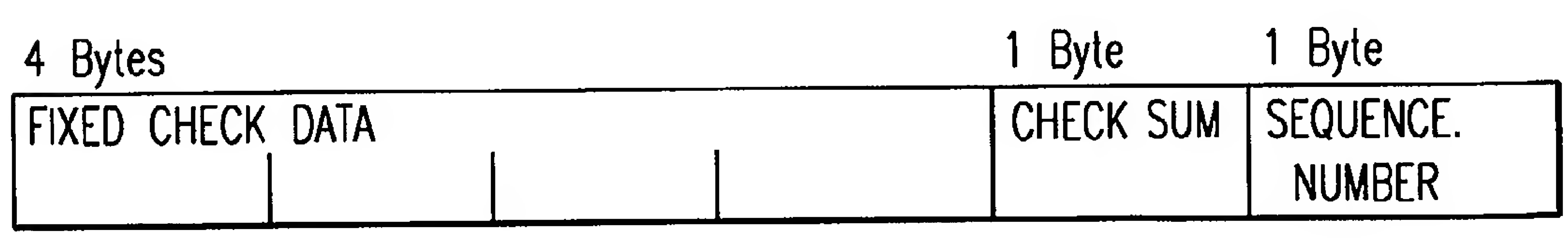

Fig. 3

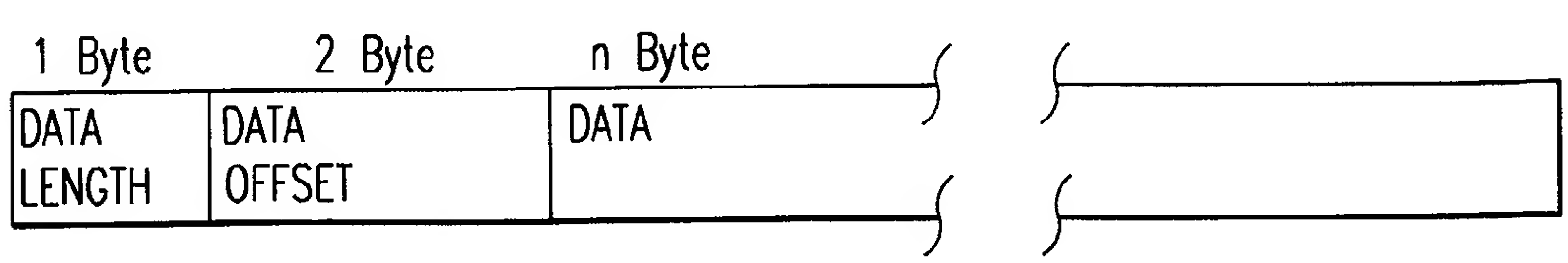

Fig. 4

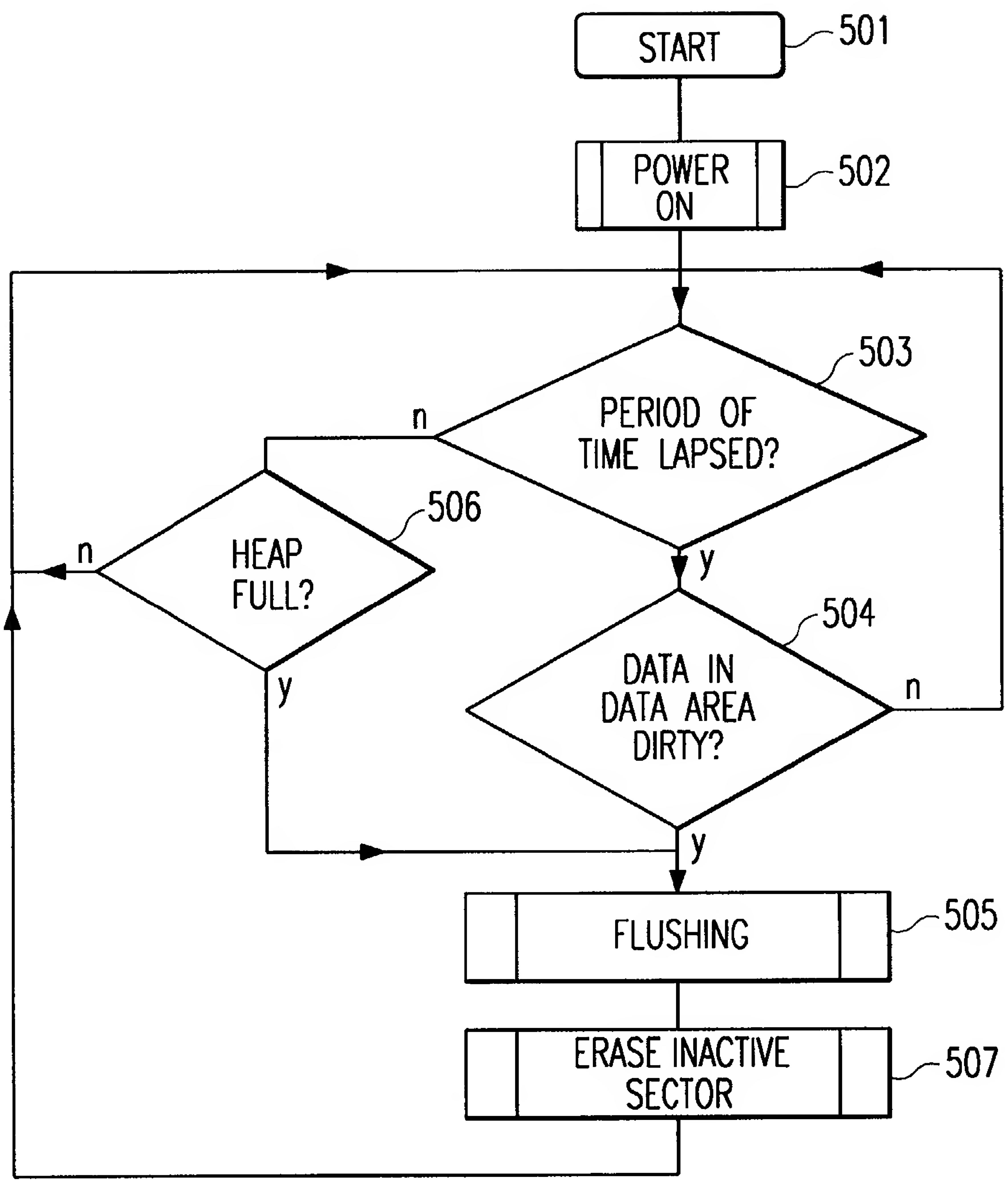
START
501
POWER ON
502
PERIOD OF TIME LAPSED?
503
n
y
HEAP FULL?
506
n
y
DATA IN DATA AREA DIRTY?
504
n
y
FLUSHING
505
ERASE INACTIVE SECTOR
507

Fig. 5

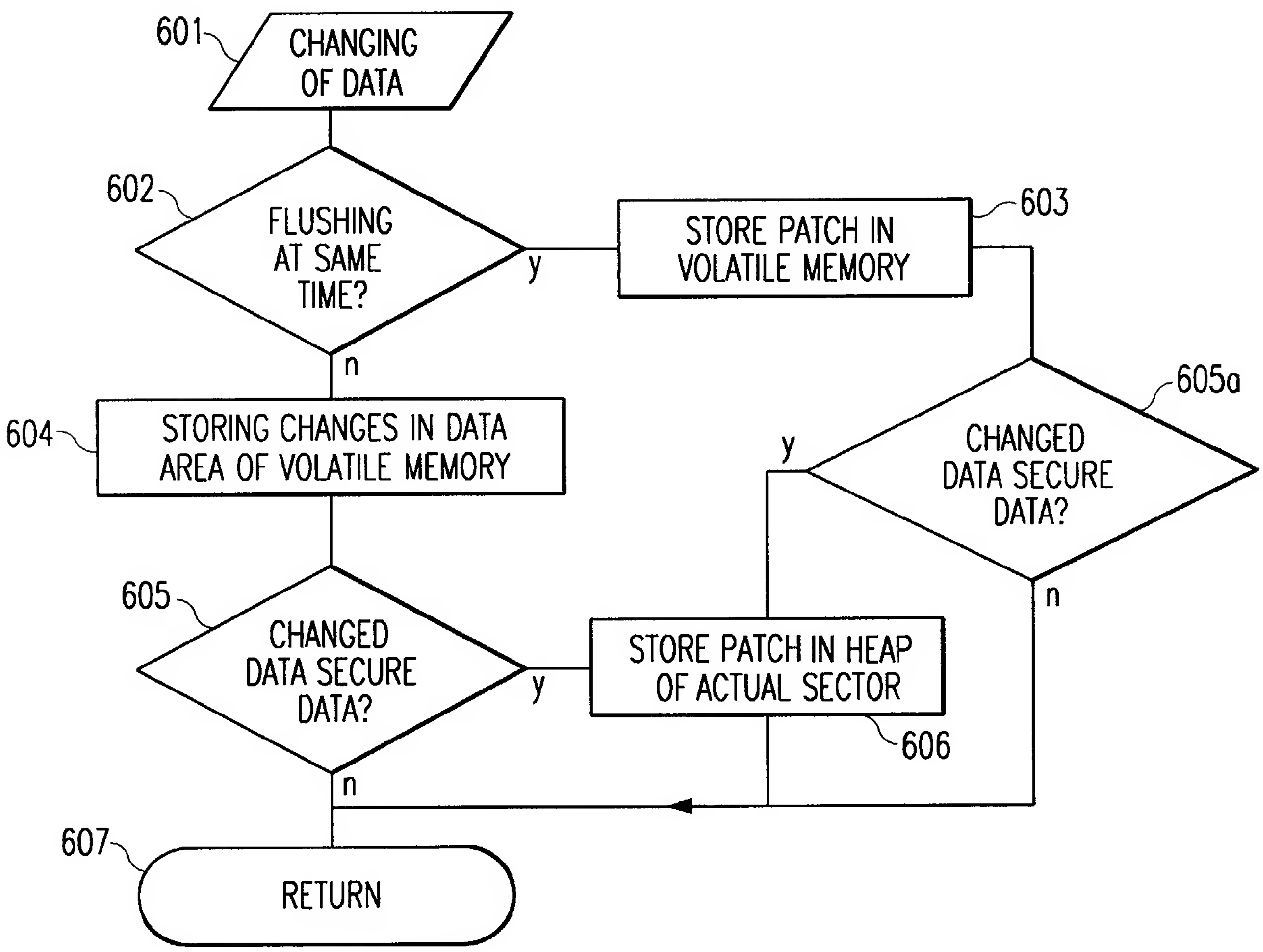
601
CHANGING OF DATA
602
FLUSHING AT SAME TIME?
y
n
603
STORE PATCH IN VOLATILE MEMORY
604
STORING CHANGES IN DATA AREA OF VOLATILE MEMORY
605a
CHANGED DATA SECURE DATA?
y
n
605
CHANGED DATA SECURE DATA?
y
n
STORE PATCH IN HEAP OF ACTUAL SECTOR
606
607
RETURN

Fig. 6

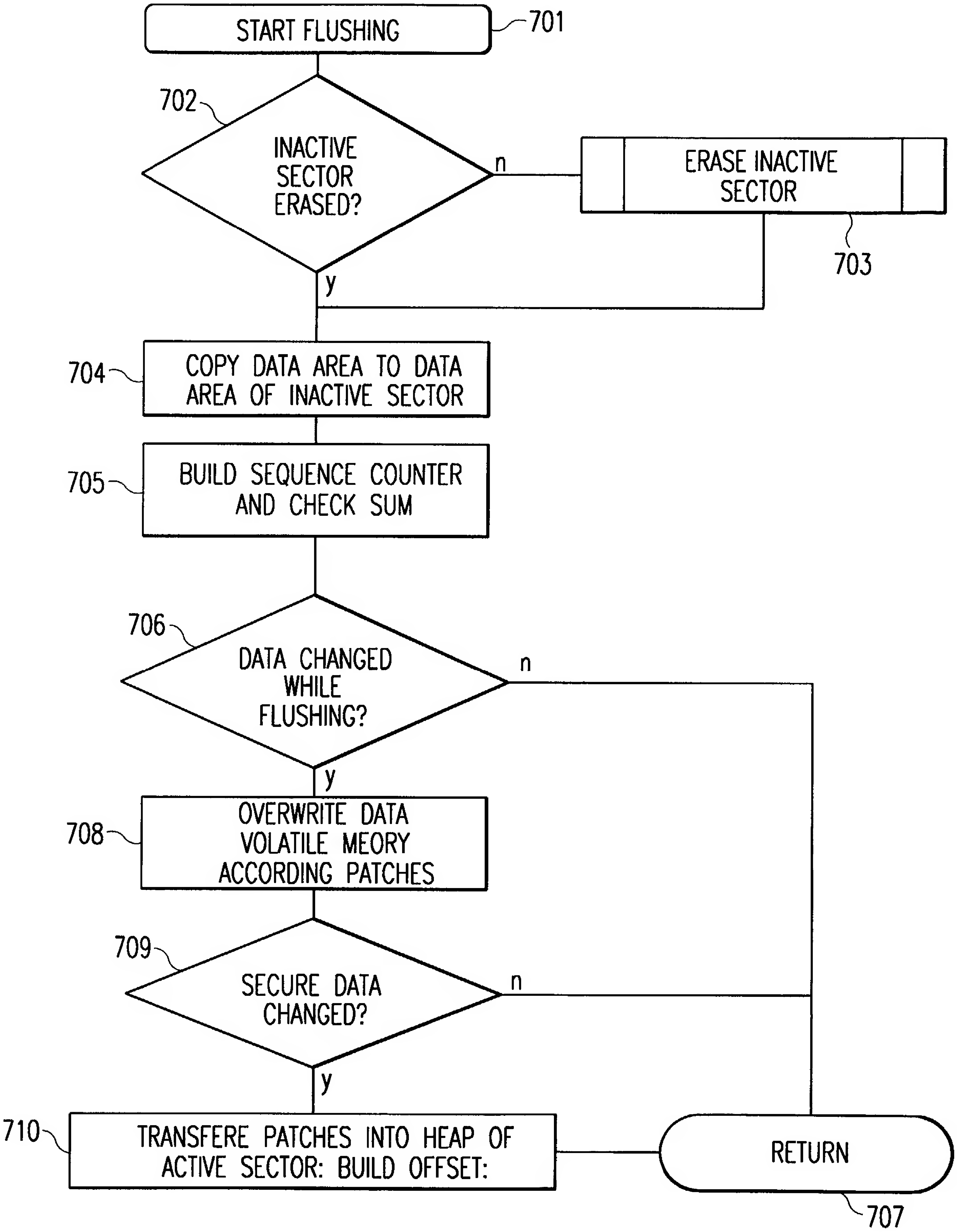
START FLUSHING
701
702
INACTIVE SECTOR ERASED?
n
ERASE INACTIVE SECTOR
703
y
704
COPY DATA AREA TO DATA AREA OF INACTIVE SECTOR
705
BUILD SEQUENCE COUNTER AND CHECK SUM
706
DATA CHANGED WHILE FLUSHING?
n
y
708
OVERWRITE DATA VOLATILE MEORY ACCORDING PATCHES
709
SECURE DATA CHANGED?
n
y
710
TRANSFERE PATCHES INTO HEAP OF ACTIVE SECTOR: BUILD OFFSET:
RETURN
707

Fig. 7

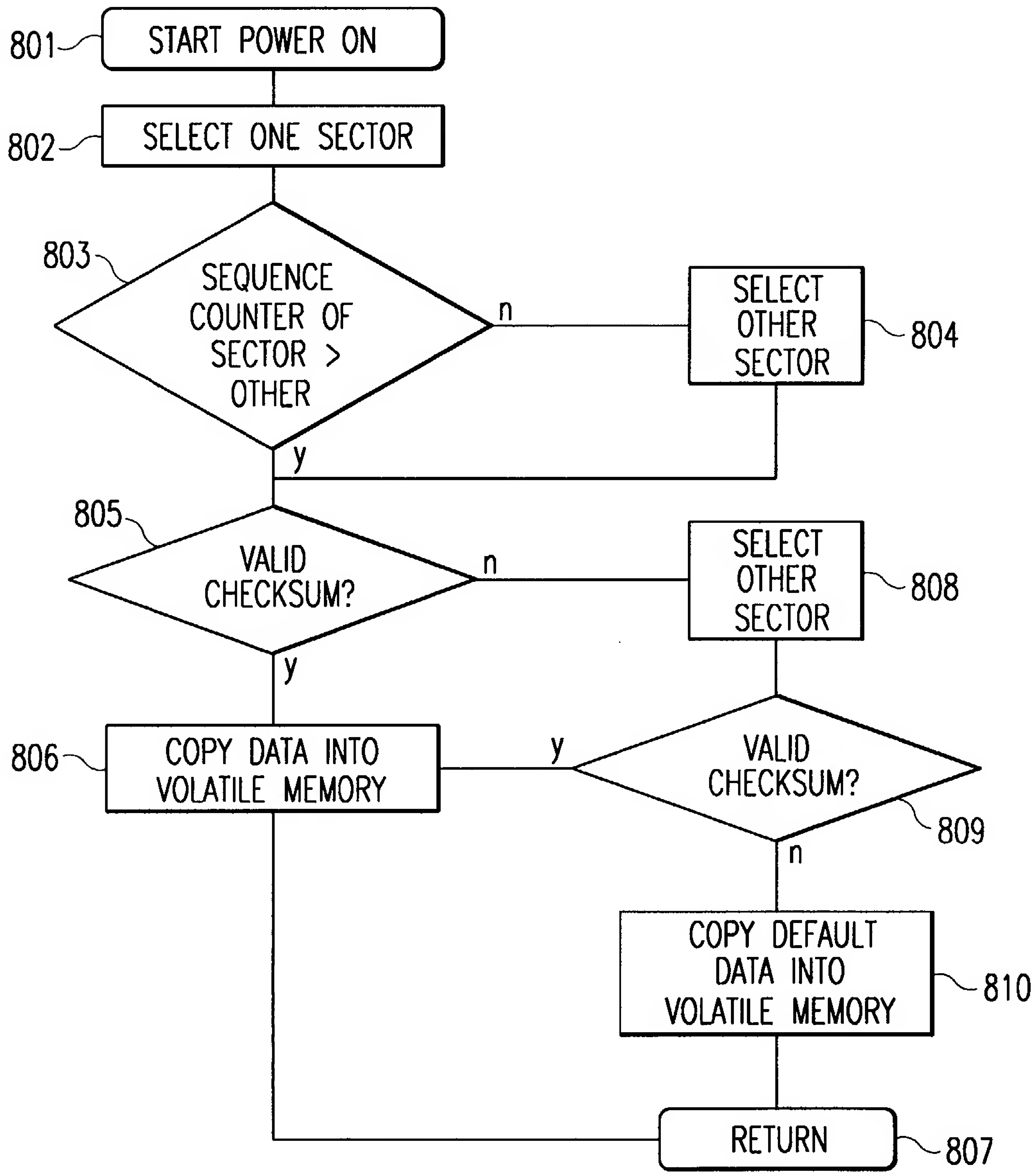
801
START POWER ON
802
SELECT ONE SECTOR
803
SEQUENCE COUNTER OF SECTOR > OTHER
n
SELECT OTHER SECTOR
804
y
805
VALID CHECKSUM?
n
SELECT OTHER SECTOR
808
y
806
COPY DATA INTO VOLATILE MEMORY
y
VALID CHECKSUM?
809
n
COPY DEFAULT DATA INTO VOLATILE MEMORY
810
RETURN
807

Fig. 8

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 11 9923

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
D,Y	EP 0 834 882 A (NOKIA MOBILE PHONES LTD) 8 April 1998 (1998-04-08)	1-4,6, 12,14, 15, 17-20,31	G06F12/02 G06F12/08
	* column 4, line 46 - column 8, line 49; figures 1-3 *		
Y	EP 1 031 929 A (HEWLETT PACKARD CO) 30 August 2000 (2000-08-30)	1-4,6, 12,14, 15, 17-20,31	
A	* the whole document *	13,16, 29,32	
A	US 5 745 425 A (ANDERSON DENNIS LEE ET AL) 28 April 1998 (1998-04-28)	1-3,6, 12,14, 15, 17-19,31	
	* column 2, line 4 - line 63 * * column 3, line 33 - column 4, line 31; figures 2,3 *		TECHNICAL FIELDS SEARCHED (Int.Cl.7)
A	DE 298 07 745 U (SIEMENS AG) 6 August 1998 (1998-08-06) * page 1, line 34 - page 2, line 33; figures 2,3 *	1,17	G06F H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	15 March 2002	Nielsen, O

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 11 9923

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

15-03-2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0834882 A	08-04-1998	GB 2317722 A	01-04-1998
		EP 0834882 A2	08-04-1998
		JP 10133940 A	22-05-1998
		US 2001002475 A1	31-05-2001
EP 1031929 A	30-08-2000	US 6104638 A	15-08-2000
		EP 1031929 A2	30-08-2000
		JP 2000250820 A	14-09-2000
		TW 446950 B	21-07-2001
US 5745425 A	28-04-1998	NONE	
DE 29807745 U	06-08-1998	DE 29807745 U1	06-08-1998

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82